eSafetyCommissioner

Monday, 13 May 2019

The Hon Suzanne (Sue) Ellery MLC
Minister for Education and Training
13th Floor, Dumas House
2 Havelock Street
WEST PERTH WA 6005
Email: Minister.Ellery@dpc.wa.gov.au

Dear Minister Ellery

I am writing to you about potential security and privacy issues relating to student email accounts. The issues have been brought to my attention by a member of the public, and appear to affect both state and independent schools in your jurisdiction.

The information we have suggests that student emails tend to be constructed using the convention firstname.lastname@education.state.gov.au (or a variation of this).

I am chiefly concerned about two risks that follow. The first is that the email naming convention permits any person, through a process of trial and error, to identify whether particular student users of the departmental education system exist.

The second risk is that other Google products, such as Google Hangouts, can be used to validate the existence of a student user within the Google Apps database by automatically validating when an email address has been correctly entered.

Both of these issues increase the likelihood that a person who presents a risk to a child might use email to initiate contact. While the obvious threat is that of a stranger with malintent, there is a risk also to children who are the subject of no-access parenting orders made by the Federal Court, or apprehended domestic violence orders that limit or prohibit contact by a parent.

I thought it may be helpful to provide some brief suggested guidance on how to manage the ease with which student user accounts may be enumerated by someone outside the school, and would be very happy to discuss the following with you.

ICT policies implemented by schools should ensure, in the interest of safeguarding students online, that products and services provided to students within the learning environment should comply with the highest safety, privacy and security standards. In particular, they should work to achieve three main objectives:

- protecting students against unauthorized access;
- protecting students from having their personally identifiable information collected; and
- promoting responsible use of the technology, including safe email practices.

User names that are easy to guess, along with their associated email addresses, are considered a security risk. Schools should consider whether it is necessary to use the firstname.lastname format, or whether another identifier could be used instead. For example, the email address might be composed of a student number, a difficult to guess combination of partial name elements, or a blend of both.

I appreciate that the current naming convention does make it easier for younger students to remember their email addresses, which is especially useful if the addresses are also used for single sign-on authentication to school platforms. The optimal solution for schools in your jurisdiction will need to balance these various considerations.

The G Suite environment, upon which Google Apps for Education is built, is designed to facilitate connections between users within a business setting. The kind of functionality that encourages connections provided via G Suite may not be appropriate where a school is concerned. For those schools using Google Apps for Education, we would recommend ICT and security personnel examine whether the configuration of the service ensures the privacy and security of students and their accounts.

Please do not hesitate to contact me if you require additional information or would like to discuss. You can also refer to our range of education and classroom resources here or refer to the Child Online Safe Organisations guidance and checklist here for ensuring technology is being utilised safely within your schools.

Kind Regards,

Julie Inman Grant
eSafety Commissioner